William B. Federman (*Admitted Pro Hac Vice*)
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
Email: wbf@federmanlaw.com

[Additional Counsel Appear on Signature Page]

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION
Lead Case No. 23-cv-4007

In re: **CUPERTINO ELECTRIC INC. LITIGATION**	**CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Kevin Crowl and Jay Wise ("Plaintiffs"), individually and on behalf of all others similarly situated ("Class Members"), bring this Consolidated Class Action Complaint action against Defendant Cupertino Electric, Inc., based on personal knowledge and on information and belief from the investigation of counsel, and allege and state as follows:

I. INTRODUCTION

1. Between June 14, 2023 and June 24, 2023, unauthorized hackers infiltrated and accessed the inadequately protected computer systems of Defendant Cupertino Electric, Inc. ("CEI", or "Defendant"). The hackers gained access to CEI's computer systems and stole, i.e., exfiltrated, the personal identifying information ("PII") of approximately 24,684 individuals whose information was negligently stored on Defendant's computer systems (the "Data Breach").

2. The PII taken by the hackers included: names, addresses, Social Security Numbers ("SSN"), driver's license numbers, and dates of birth (collectively, "PII"). Essentially everything a bad actor needs to steal a person's identity and cause harm.

3. Subsequently, on July 12, 2023, Defendant determined that the PII stolen in the Data Breach was PII from employees "working at CEI between January 21, 1954 and June 23, 2023."[1] No explanation was provided for why Defendant stored this information back to 1954.

4. In short, considering Defendant negligently failed to protect Plaintiffs' and Class Members' PII and unnecessarily retained such PII for approximately 70 years, cyber

[1] *See* **Exhibit 1**.

criminals were able to steal everything they could possibly need to commit nearly every conceivable form of identity theft and wreak havoc on the financial and personal lives of Plaintiffs and Class Members.

5. Defendant's failure to implement adequate and reasonable measures to ensure their computer systems were protected, failing to delete Plaintiffs' and Class Members' PII since its inception, failing to take adequate steps to prevent and stop the breach, failing to timely detect the breach, failing to disclose the material facts that they did not have adequate computer systems and security practices to safeguard the PII, failing to honor their repeated promises and representations to protect Plaintiffs' and Class Members' PII, and failing to provide timely and adequate notice of the Data Breach has caused substantial harm and injuries to Plaintiffs and Class Members across the United States.

6. As a result of the Data Breach, Plaintiffs and Class Members have already suffered actual, concrete damages in the form of identity theft and fraudulent charges. In addition, Plaintiffs and Class Members have spent many hours cancelling credit card accounts, filing police reports, and monitoring credit reports and credit and bank accounts to combat identity theft. Many are now paying monthly or annual fees for identity theft and credit monitoring services. Now that their PII has been released into the criminal cyber domains, Plaintiffs and Class Members must spend their time being extra vigilant due to Defendant's failures to prevent being victimized for the rest of their lives.

7. Plaintiffs bring this class action lawsuit on behalf of a nationwide class to hold Defendant responsible for its negligent and reckless failure to use reasonable, current cybersecurity measures to protect Class Members' PII.

8. Because Defendant presented such a soft target to cybercriminals, Plaintiffs and Class Members have experienced actual misuse of their PII and are exposed to a heightened and imminent risk of future fraud and identity theft. Plaintiffs and Class Members must now and in the future, take their time to more closely monitor their financial accounts to guard against additional instances of identity theft and fraud.

9. Plaintiffs and Class Members have also incurred out-of-pocket costs for, among other things, purchasing credit monitoring services, implementing credit freezes, obtaining credit reports, cancelling credit card accounts, and other protective measures to deter and detect identity theft.

10. On behalf of themselves and all others similarly situated, Plaintiffs seek actual damages, statutory damages, and punitive damages, with attorney fees, costs, and expenses under Cal. Civ. Code § 56, consumer protection and unfair and deceptive practices acts, negligence, negligence per se, unjust enrichment, and breach of implied contract. Plaintiffs also seek injunctive relief, including significant improvements to Defendant's data security systems, future annual audits, long-term credit monitoring services funded by Defendant, and other remedies as the Court sees fit.

II. THE PARTIES

11. Plaintiff Kevin Crowl is a citizen and a resident of Douglas County, Nebraska, and is a former employee of CEI who worked for Defendant from July 6, 2021

to August 18, 2021.

12. Plaintiff Jay Wise is a citizen and a resident of the State of Texas and is a former employee of CEI who worked for Defendant from September 2019 through June 2020.

13. Defendant is a Delaware corporation with its principal place of business in San Jose, California, in Santa Clara County.

III. JURISDICTION AND VENUE

14. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

15. This Court has diversity jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendant, including the Plaintiffs.

16. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, it regularly transacts business in this District, and many Class Members reside in this District.

17. Venue as to Defendant is proper in this judicial district under 28 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District and many of Defendant's acts complained of herein occurred within this District.

IV. FACTUAL ALLEGATIONS

18. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

19. Defendant is relied upon to design and execute "first-of-their-kind" electrical systems for corporations, public entities, utility companies, and developers. Defendant has offices throughout California and jobsites across the United States to deliver electrical services for commercial, energy, and data center customers.[2]

20. In the ordinary course of business, Defendant stores, maintains, and uses Plaintiffs' and Class Members' PII, including but not limited to:

a. Names,

b. Addresses,

c. Social Security numbers,

d. Driver's license numbers, and

e. Dates of birth.

21. Defendant understands the importance of securely maintaining PII.

22. In fact, as discussed below, Defendant's Privacy Policy emphasizes its commitment to protecting the PII of Plaintiffs and Class Members.

A. The Data Breach

[2] https://www.cei.com/about-cei

23. On or around July 28, 2023, CEI began sending Plaintiffs and Class Members a Notice of Security Incident letter (the "Notice") providing, for the first time, a public notice of "an incident that may affect the privacy of some of your information."[3]

24. In the Notice, CEI notified certain office and field employees that on June 24, 2023—over a month earlier—it had "became aware of suspicious activity on certain internal systems" and, after an internal investigation, "determined that an unauthorized third party ***accessed and acquired*** information on certain CEI systems between June 14, 2023 and June 24, 2023". It went on to say that within eighteen (18) days of this discovery, CEI confirmed "that the confidentiality of personal data of certain office and field employees working at CEI between January 21, 1954 and June 23, 2023 was impacted in this incident."[4]

25. Yet, despite knowing many former and current employees' PII was in danger, Defendant did nothing to warn Plaintiffs and Class Members until over a month later. During this time, the cyber criminals had free reign to defraud their unsuspecting victims and, in fact, did defraud Plaintiffs and Class Members. CEI apparently chose to complete its internal investigation and develop its excuses and speaking points before giving Plaintiffs and Class Members the information they needed to protect themselves against fraud and identity theft.

26. Defendant also failed to explain why it has departed from reasonable data retention best practices and has ***never*** deleted former employees' PII dating as far back as

[3] *See* **Exhibit 1**; **Exhibit 2**.

[4] *Id*.

1954. Retaining Plaintiffs' and Class Members' PII for such an unnecessary length of time contradicts data retention best practices, which advises that "data should only be kept as long as it's useful."[5] It is inconceivable how PII dating back to 1954 is somehow useful in 2023.

27. Further, after its "comprehensive and thorough review," Defendant finally informed Plaintiffs and Class Members that:

> The information impacted by this incident may include your name, address, Social Security Number (SSN), driver's license number, and date of birth.

This was a staggering coup for the cyber criminals and a stunningly bad showing for Defendant.

28. In spite of the severity of the Data Breach, Defendant has done very little to protect Plaintiffs and Class Members. In the Notice, CEI states that it is notifying Plaintiffs and Class Members of "resources available to [them] to help protect [their] information from possible misuse, *should [they] feel it is appropriate to do so.*"[6] In effect, shirking its responsibility for the harm it has caused and putting it all on the victims.

29. Defendant CEI failed to adequately safeguard Plaintiffs' and Class Members' PII, allowing the cyber criminals to exfiltrate this wealth of priceless information for over a month before CEI warned the Plaintiffs and Class Members to be on the lookout.

[5] https://www.intradyn.com/data-retention-policy/

[6] *Id.*

30. Defendant failed to spend sufficient resources on monitoring external incoming emails and training its employees to identify email-born threats and defend against them.

31. Defendant had obligations created by reasonable industry standards, its own contracts with its customers and employees, common law, and its representations to Class Members to retain their PII in compliance with all applicable laws governing the retention of their personal data.

32. Plaintiffs and Class Members provided their PII to CEI with the reasonable expectation and mutual understanding that CEI would comply with its obligations to keep such information confidential and secure from unauthorized access.

33. Indeed, as discussed below, CEI promised its former and current employees that it would do just that.

B. Defendant Promised to Protect PII

34. CEI provides all former and current employees, including Plaintiffs, its CPRA (California Privacy Rights Act of 2020) External Privacy Policy. In fact, CEI is required to do so by federal and state law. CEI's CPRA External Privacy Policy states, as relevant:

> CEI's privacy commitments are fundamental to the way we run our business. These commitments apply to everyone who has a relationship with CEI….Cupertino Electric is committed to providing you with the best overall experience in our services. We strive to strike the right balance between using your

> personal data to ensure the quality of those experiences and protecting your privacy.[7]

35. While CEI claims it is committed to protecting the privacy of "everyone who has a relationship with CEI", the Data Breach and unnecessary retention of PII proves otherwise.

36. If CEI truly understands the importance of safeguarding its current and former employees PII, it should compensate the Plaintiffs and Class Members for their losses, provide long-term protection for the Class, and agree to Court-ordered and enforceable changes to its cybersecurity policies, data retention procedures, and adopt regular and intensive training to ensure that something like this never happens again.

37. The Plaintiffs' and Class Members' PII is now in the hands of cyber criminals who have already actually misused such PII in the form of identity theft and fraud. Considering Plaintiffs and Class Members have already experienced actual misuse of their PII, coupled with the sensitive nature of the PII stolen, Plaintiffs and Class Members are currently suffering from an imminent and substantial risk of future identity theft and fraud.

C. Defendant had an Obligation to Protect PII under Federal and State Law and the Applicable Standard of Care

38. Defendant is prohibited by the Federal Trade Commission Act (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." By allowing an unknown third-party to access a CEI server and steal Plaintiffs' and Class

[7] Cupertino Electric, Inc., "CPRA External Privacy Policy," Effective Date: June 30, 2023, https://www.cei.com/privacy-policy (last accessed January 29, 2024).

Members' PII, CEI failed to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data. CEI's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

39. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making. [8]

40. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[9] Among other things, the guidelines note businesses should properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of

[8] *See* Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited January 29, 2024).

[9] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited January 29, 2024).

data being transmitted from the system; and have a response plan ready in the event of a breach.[10]

41. In addition to their obligations under federal and state laws, Defendant owed a duty to Plaintiffs and Class Members whose PII was entrusted to Defendant to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the PII of the Plaintiffs and Class Members.

42. Defendant owed a duty to Plaintiffs and Class Members whose PII was entrusted to Defendant to design, maintain, and test its computer systems and email system to ensure that the PII in Defendant's possession was adequately secured and protected.

43. Defendant owed a duty to Plaintiffs and Class Members whose PII was entrusted to Defendant to create and implement reasonable data security practices and procedures to protect the PII in their possession, including adequately training its employees and others who accessed PII within its computer systems on how to adequately protect PII.

44. Defendant owed a duty to Plaintiffs and Class Members whose PII was entrusted to Defendant to implement processes that would detect a breach on its data

[10] *Id.*

security systems in a timely manner.

45. Defendant owed a duty to Plaintiffs and Class Members whose PII was entrusted to Defendant to act upon data security warnings and alerts in a timely fashion.

46. Defendant owed a duty to Plaintiffs and Class Members whose PII was entrusted to Defendant to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust PII with Defendant.

47. Defendant owed a duty to Plaintiffs and Class Members whose PII was entrusted to Defendant to disclose in a timely and accurate manner when data breaches occurred.

48. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

49. As a result of the Data Breach, Defendant breached the above-mentioned duties owed to Plaintiffs and Class Members.

D. Cyber Criminals Will Continue to Use Plaintiffs' and Class Members' PII to Defraud

50. PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been and will continue to be misused in a variety of ways by criminals to exploit Plaintiffs and the Class Members and profit off their misfortune.

51. Each year, identity theft causes tens of billions of dollars of losses to victims

in the United States.[11] For example, with the PII stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[12]

52. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of PII in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[13]
>
> [Emphasis added.]

53. This was a financially motivated Breach, as the only reason the cyber criminals go through the trouble of running a targeted cyberattack against companies like CEI is to get information that they can monetize by selling it on the black market/Dark

[11] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[12] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[13] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

Net or Web for use in the kinds of criminal activity described herein. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[14] "[I]f there is reason to believe that your PII has been stolen, you should assume that it can end up for sale on the dark web."[15]

54. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

55. For instance, with a stolen social security number, which is part of the PII compromised here, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits. [17]

56. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.

---

[14] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[15] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[16] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* GAO, June 4, 2007, https://www.gao.gov/assets/gao-07-737.pdf

[17] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

57. Defendant's offer of twenty-four (24) months of credit and identity monitoring to Plaintiffs and the Class is woefully inadequate and will not fully protect them from the damages and harm caused by Defendant's cybersecurity failures. While some Plaintiffs and Class Members have already experienced actual misuse of their PII, the full scope of the harm has yet to be realized. There may be a time lag between when additional harm occurs versus when it is discovered, and between when the PII is stolen and when it is used. Once the twenty-four months have expired, Plaintiffs and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to Defendant's gross negligence. Furthermore, identity monitoring only alerts someone to the fact that they have *already been the victim of identity theft*—it does not prevent identity theft.[18] Nor can identity monitoring services remove PII from the dark web.[19] "The people who trade in stolen PII [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[20]

58. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have experienced actual misuse of their PII and, as a result, have been placed at an imminent, immediate, and continuing increased risk of harm of continued fraud and identity theft. Plaintiffs and Class Members must now take the time and effort to mitigate

[18] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html.

[19] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[20] *Id.*

the actual and potential impact of the Data Breach in their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Even more seriously is the identity restoration that Plaintiffs and other Class Members must go through, which can include spending countless hours filing police reports, filling out IRS forms, Federal Trade Commission checklists, Department of Motor Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiffs and Class Members must take.

59. Plaintiffs and Class Members have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Actual misuse of the PII in the forms of identity theft and fraud;

b. Trespass, damage to, and theft of their personal property including their PII;

c. Improper disclosure of their PII;

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their PII and that identity thieves may use that information to defraud other victims of the Data Breach;

f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach; and

g. Ascertainable losses in the form of deprivation of the value of Plaintiffs' and Class Members' PII for which there is a well-established and quantifiable national and international market.

60. Plaintiffs and Class Members have an interest in ensuring that their information, which remains in the possession of the Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown itself to be wholly incapable of protecting Plaintiffs' and Class Members' PII.

61. Defendant acknowledged the harm caused by the Data Breach because it offered Plaintiffs and Class Members the woefully inadequate twenty-four months of identity theft repair and credit monitoring services. Twenty-four months of credit and identity theft monitoring is, however, inadequate to protect Plaintiffs and Class Members from a lifetime of identity theft risk.[21]

62. Defendant further acknowledged, in its letter to Plaintiffs and Class Members, that CEI needed to improve its security protocols, stating: "As part of our ongoing commitment to the privacy of information in our care at CEI, we are reviewing our policies, procedures, and processes related to the storage and access of personal

[21] *See* **Exhibit 1**.

information to reduce the likelihood of a similar future event."[22]

63. The Notice further acknowledged that the Data Breach would cause Plaintiffs and the Class Members inconvenience, and that financial harm would likely occur by stating: "We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months."[23]

64. At Defendant's suggestion, Plaintiffs and Class Members are desperately trying to mitigate the damage that the Data Breach has caused them. Given the kind of PII Defendant made accessible to hackers, the Plaintiffs and Class Members are certain to incur additional damages. Because identity thieves have their PII, Plaintiffs and Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[24]

65. None of this should have happened.

E. Defendant Was Aware of the Risk of Cyber Attacks

66. Defendant, who collects employees' and customers' PII requiring the collection and maintenance of highly sensitive and valuable PII, should have been aware,

[22] *Id.*

[23] *Id.*

[24] *Will a New Social Security Number Affect Your Credit?*, Lexington Law (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

and indeed was aware, that it was at risk for a data breach that could expose the PII that it collected and maintained.

67. With the increasing prevalence of data breach announcements, Defendant certainly recognized it had a duty to use reasonable measures to protect the wealth of PII that it collected and maintained.

68. In 2022, a total of 1,802 data breaches occurred, which represents the second highest number of data events in a single year and just 60 events short of the all-time record of 1,862 in 2021.

69. In 2022, the utility services industry saw 115 data breaches with 467,664 victims.[25] In light of the significant number of data breaches that occurred in the utility services industry in 2022, Defendant knew or should have known that its employees' PII would be targeted by cybercriminals.

70. Defendant was clearly aware of the risks it was taking and the harm that could result from inadequate data security and its non-existent data management procedures.

F. Defendant Could Have Prevented the Breach

71. Data breaches are preventable.[26] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred

[25] https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf.

[26] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* Data Breach and Encryption Handbook (Lucy Thompson, ed., 2012).

could have been prevented by proper planning and the correct design and implementation of appropriate security solutions.[27] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[28]

72. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[29]

73. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks. [30]

74. The guidelines establish that businesses should protect the confidential information that they keep; develop a written records retention policy to identify what information must be kept and for how long; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches

[27] *Id*. at 17.

[28] *Id*. at 28.

[29] *Id*.

[30] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business

to correct security problems. The guidelines also recommend that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[31]

75. Upon information and belief, Defendant failed to maintain reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, Defendant also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity preparation.

76. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection." [32]

77. Further, to prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

[31] *Id*.

[32] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

a. **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.

b. **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).

c. **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

d. **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it.

e. **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the

sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

f. **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

g. **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.[33]

78. In addition, to prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following the measures:

a. **Secure internet-facing assets**

i. Apply latest security updates

ii. Use threat and vulnerability management

[33] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001.

iii. Perform regular audit; remove privileged credentials

b. **Thoroughly investigate and remediate alerts**

i. Prioritize and treat commodity malware infections as potential full compromise;

c. **Include IT Pros in security discussions**

i. Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

d. **Build credential hygiene**

i. Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

e. **Apply principle of least-privilege**

i. Monitor for adversarial activities

ii. Hunt for brute force attempts

iii. Monitor for cleanup of Event Logs

iv. Analyze logon events

f. **Harden infrastructure**

i. Use Windows Defender Firewall

ii. Enable tamper protection

iii. Enable cloud-delivered protection

iv. Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[34]

79. Given that Defendant was storing the PII of thousands of individuals for the past seventy (70) years, Defendant could and should have implemented all of the above measures to prevent and detect cyber-attacks.

80. Specifically, among other failures, Defendant had far too much confidential unencrypted information held on its systems. Such PII should have been segregated into an encrypted system.[35]

81. Moreover, it is well-established industry standard practice for a business to dispose of confidential PII once it is no longer needed. The FTC, among others, has repeatedly emphasized the importance of disposing unnecessary PII, saying simply: "Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not on your system, it can't be stolen by hackers."[36]

82. Defendant, rather than following this basic standard of care, kept

[34] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

[35] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, Aug. 14, 2018, https://www.digitalguardian.com/blog/how-safeguard-your-business-data-encryption

[36] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf at p. 6.

individuals' unencrypted PII indefinitely. The Notice stated, "On July 23, 2023 we determined that the confidentiality of personal data of certain office and field employees working at CEI between January 21, 1954 and June 23, 2023 was impacted in this incident."[37] CEI was founded in 1954.[38]

83. In sum, this Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all PII. Further, the scope of the Data Breach could have been dramatically reduced had Defendant utilized proper record retention and destruction practices.

V. PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

84. Plaintiffs and the Class have been damaged by the targeted cyber-attack resulting in the theft of their PII in the Data Breach.

85. As a result of the targeted cyber-attack compromising Plaintiffs' and Class Members' PII, which includes highly confidential information such as Social Security numbers, Plaintiffs and Class Members have experienced actual misuse of their PII and are presently at a substantial risk for additional instances of identity theft or fraud in the future.

86. Plaintiffs and the Class also presently face a substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

87. Plaintiffs and the Class have been, and currently face substantial risk of

[37] *See* **Exhibit 1**.

[38] *See* https://www.cei.com/about-cei/history

being targeted now and in the future, to phishing, data intrusion, and other illegality based on their PII being compromised in the Data Breach as potential fraudsters could use the information garnered to target such schemes more effectively against Plaintiffs and the Class.

88. Plaintiffs and the Class may incur additional out-of-pocket costs for implementing protective measures such as purchasing credit monitoring fees, cancelling credit card accounts, credit report fees, credit freeze fees, and other similar costs directly or indirectly related to mitigating the Data Breach.

89. Plaintiffs and the Class also suffered a loss in value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in data breach cases.

90. Plaintiffs and the Class have spent and will continue to spend significant amounts of time monitoring their financial accounts, cancelling their financial accounts, and monitoring their credit scores and records for misuse.

91. Plaintiffs and the Class have already suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of identity theft and fraud, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

92. Moreover, Plaintiffs and the Class have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of proper and adequate security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing

personal and financial information is not accessible online and that access to such data is password protected.

93. Further, as a result of Defendant's conduct, Plaintiffs and the Class are forced to live with the anxiety that their PII—which contains the most intimate details about a person's life—may be disclosed to the entire world, whether physically or virtually, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

94. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and the Class have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm because of the Data Breach.

A. Plaintiff Kevin Crowl

95. Plaintiff Crowl received Defendant's Notice letter from Defendant by mail on or around July 28, 2023, over a month after the Data Breach occurred on June 14, 2023.

96. The Notice advised him that the PII compromised in the Data Breach included Plaintiff Crowl's name, address, Social Security number, driver's license number, and date of birth.[39]

97. Plaintiff Crowl entrusted his PII and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents would take industry-standard precautions to protect, maintain, and safeguard that information from theft and disclosure, and would timely notify him of any data security

[39] *See* **Exhibit 1.**

incidents related to his PII. Plaintiff Crowl would not have allowed Defendant to collect and maintain his PII had he known that Defendant would not take reasonable steps to safeguard his PII.

98. As a direct and traceable result of the Data Breach, Plaintiff Crowl has experienced actual misuse of his PII in the form of identity theft and fraud. Specifically, in August of 2023, Plaintiff Crowl made a credit card fraud claim with his bank, First National Bank of Omaha, for fraudulent charges appearing on his credit card account dated after the Data Breach occurred on June 14, 2023. Subsequently, on August 6, 2023, Plaintiff Crowl received a letter from the First National Bank of Omaha Fraud Department informing him that, after conducting an investigation, the post-breach transactions appearing on his credit card account were fraudulent.

99. Following the fraudulent charges to his credit card, Plaintiff Crowl spent hours mitigating the damages he suffered from the identity theft and fraud by filing a credit card fraud claim with the First National Bank of Omaha, disputing the fraudulent charges, spending time on telephone calls to remove the fraudulent charges, cancelling his credit card account, and opening a new credit card account.

100. In addition, as a direct and traceable result of the Data Breach, Plaintiff Crowl has received hundreds of spam emails and text messages since the Data Breach occurred on June 14, 2023. Plaintiff Crowl has also spent hours addressing and deleting the hundreds of spam emails and text messages he has received since the Data Breach occurred.

101. The time Plaintiff Crowl has been forced to spend dealing with and responding to the direct consequences of the Data Breach is time that has been lost forever and cannot be recaptured.

102. Considering Plaintiff Crowl's PII has already been misused to commit identity theft and credit card fraud, Plaintiff Crowl has also suffered actual damages because he is at an imminent, impending, and substantial risk for additional identity theft and future economic harm.

103. Plaintiff Crowl stores all documents containing his PII in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for the online accounts that he has.

104. Plaintiff Crowl has also suffered actual injury in the form of damages to, and diminution in, the value of his PII – a form of intangible property that Plaintiff Crowl entrusted to Defendant. This PII was compromised, and its value has been diminished because of the Data Breach.

105. Plaintiff Crowl has suffered actual damages and is at an imminent, impending, and substantial risk for identity theft and future economic harm due to the highly sensitive nature of the information that was targeted and stolen in the Data Breach, especially his Social Security number, in combination with his name.

106. Knowing that thieves stole his PII in a targeted cyber-attack and knowing that his PII will likely be sold on the dark web has caused Plaintiff Crowl great anxiety.

107. Additionally, Plaintiff Crowl does not recall having been involved in any other data breaches in which his highly confidential PII, such as his Social Security number, was compromised.

108. Plaintiff Crowl has a continuing interest in ensuring that his PII, which remains in the possession of Defendant, is protected and safeguarded from future data breaches.

109. As a result of the Data Breach, Plaintiff Crowl is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, and other forms of fraud for years to come.

B. Plaintiff Jay Wise

110. Plaintiff Wise received Defendant's Notice letter from Defendant by mail on or around July 28, 2023, over a month after the Data Breach occurred on June 14, 2023.

111. Plaintiff Wise was employed by Defendant from September 2019 through June of 2020.

112. The Notice advised him that the PII compromised in the Data Breach included Plaintiff Wise's name, address, Social Security number, driver's license number, and date of birth.[40]

113. Prior to this Data Breach, Plaintiff Wise had taken steps to keep his PII safe and has monitored his PII closely. He has not knowingly transmitted his PII over unsecured or unencrypted internet connections.

[40] *See* **Exhibit 2.**

114. Plaintiff Wise has suffered actual damages and is at an imminent, impending, and substantial risk for identity theft and future economic harm due to the highly sensitive nature of the information that was targeted and stolen in the Data Breach. Since learning about the breach, in an effort to mitigate the risk, Plaintiff Wise has spent time and effort reviewing financial statements and identity theft protection reports to detect and prevent identity theft. Plaintiff Wise has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the theft and compromise of his PII. Plaintiff Wise will continue to spend additional time and incur future economic costs associated with the detection and prevention of identity theft.

115. Plaintiff Wise entrusted his PII and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to his PII. Plaintiff Wise would not have allowed Defendant to collect and maintain his PII had he known that Defendant would not take reasonable steps to safeguard his PII.

116. Plaintiff Wise has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on telephone calls, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This is time that has been lost forever and cannot be recaptured.

117. Plaintiff Wise stores all documents containing his PII in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for the online accounts that he has.

118. Plaintiff Wise has suffered actual injury in the form of damages to, and diminution in, the value of his PII – a form of intangible property that Plaintiff Wise entrusted to Defendant. This PII was compromised, and its value has been diminished as a result of the Data Breach.

119. Plaintiff Wise has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

120. Plaintiff Wise has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII resulting from the compromise of his PII in the targeted Data Breach, especially his Social Security number in combination with his name, address, and date of birth.

121. Additionally, Plaintiff Wise does not recall having been involved in any other data breaches in which his highly confidential PII, such as Social Security Number was compromised.

122. Plaintiff Wise has a continuing interest in ensuring that his PII, which remains in the possession of Defendant, is protected and safeguarded from future data breaches.

123. As a result of the Data Breach, Plaintiff Wise is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

VI. CLASS ALLEGATIONS

124. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

125. Plaintiffs bring this class action on behalf of a Nationwide Class according to Federal Rules of Civil Procedure, Rules 23(b)(2), 23(b)(3), and 23(b)(4).

126. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> **All natural persons residing in the United States whose personal identifiable information (PII) was compromised as a result of the Data Breach suffered by Defendant between June 14, 2023 and June 24, 2023 and announced by Defendant on or about July 28, 2023.**

127. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

A. CLASS CERTIFICATION IS APPROPRIATE

128. The proposed Nationwide Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

129. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. According to the Attorney General for the State of Maine Data Brech

Notifications, the total number of persons affected by the Data Brech is 24,684.

130. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. When Defendant actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendant failed to adequately safeguard Plaintiffs' and Class Members' PII;

c. Whether Defendant owed a duty to Plaintiffs and the Class to adequately protect their PII, and whether it breached this duty;

d. Whether Defendant breached its duties to Plaintiffs and the Class as a result of the Data Breach;

e. Whether Defendant failed to provide adequate cyber security;

f. Whether Defendant knew or should have known that its computer and network security systems were vulnerable to cyber-attacks;

g. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its company network;

h. Whether Defendant was negligent in permitting unencrypted PII off vast numbers of individuals to be stored within its network since its inception in 1954;

i. Whether Defendant was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach to include former employees and business associates;

j. Whether Defendant breached implied contractual duties to Plaintiffs and Class Members to use reasonable care in protecting their PII;

k. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and Class Members;

l. Whether Defendant continues to breach duties to Plaintiffs and Class Members;

m. Whether Plaintiffs and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

n. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief; and

o. Whether Defendant's actions alleged herein constitute gross negligence, and whether Plaintiffs and Class Members are entitled to punitive damages.

131. **Typicality:** Plaintiffs' claims are typical of the claims of the members of the Class. Plaintiffs and the members of the Class sustained damages as a result of Defendant's

uniform wrongful conduct. All had their PII compromised and stolen as a result of the Data Breach.

132. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests of the Class. Plaintiffs have retained counsel competent and experienced in complex litigation and class actions. Plaintiffs have no interests antagonistic to those of the Class, and there are no defenses unique to Plaintiff. Plaintiffs and his counsel are committed to prosecuting this action vigorously on behalf of the members of the Class and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Class.

133. **Risks of Prosecuting Separate Actions:** This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendant or would be dispositive of the interests of members of the proposed Class. Furthermore, Defendant is still in possession of PII of the Plaintiffs and the Class, and Defendant's systems are still vulnerable to attack—one standard of conduct is needed to ensure the future safety of PII in Defendant's possession.

134. **Policies Generally Applicable to the Class:** This case is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Plaintiffs and the Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class, and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendant's practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiffs' challenge to those practices hinge on Defendant's conduct with

respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiffs.

135. **Superiority:** This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiffs and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendant's conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendant. Even if members of the Class could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

VII. CAUSES OF ACTION

A. COUNT I – NEGLIGENCE

136. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

137. As a condition of their employment, Plaintiffs and Class Members were obligated to provide Defendant with their PII.

138. Upon accepting and storing the PII of Plaintiffs and the Class Members on its computer systems and networks, Defendant undertook and owed a duty to Plaintiffs

and Class Members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII was wrongfully disclosed. Plaintiffs and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class Members had no ability to protect their PII that was in Defendant's possession. As such, a special relationship existed between Defendant, the Plaintiff, and the Members of the Class.

139. Because of this special relationship, Defendant required Plaintiffs and Class Members to provide their PII, including names, Social Security numbers, and other personal information.

140. Defendant knew, or should have known, of the risks inherent in collecting and storing this PII of the Plaintiffs and the Class and the importance of adequate security.

141. Implied in these exchanges was a promise by Defendant to ensure that the PII of the Plaintiffs and Class Members in its possession was only used to provide the agreed-upon compensation and other employment benefits from Defendant and that Defendant would destroy any PII that it was not required to maintain.

142. Through Defendant's acts and omissions, including Defendant's failure to provide adequate security, its failure to protect Plaintiffs' and Class Members' PII from being foreseeably accessed, and its improper retention of PII it was not required to maintain, Defendant negligently failed to observe and perform its duty.

143. Defendant was aware of the fact that cyber criminals routinely target large corporations through cyberattacks in an attempt to steal customer and employee PII.

144. Defendant owed Plaintiffs and the Class Members a common law duty to use reasonable care to avoid causing foreseeable risks of harm to Plaintiffs and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard or delete such data and providing notification to Plaintiffs and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

145. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. See Restatement (Second) of Torts § 302B.

146. Defendant owed duties of care to Plaintiffs and the Class whose PII was entrusted to it. Defendant's duties included the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession;

b. To exercise reasonable care in deleting data that is no longer needed;

c. To protect the PII in its possession using reasonable and adequate security procedures and systems;

d. To adequately and properly train its employees regarding how to properly and securely transmit and store PII;

e. To implement processes to quickly detect a data breach, security incident, or intrusion; and

f. To promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

147. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent considering the foreseeable risks and known threats.

148. As a direct and proximate result of Defendant's negligent conduct, including but not limited to its failure to implement and maintain reasonable security practices and procedures as described above, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

149. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the PII of Plaintiffs and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and Class Members while it was within Defendant's possession and control.

150. In addition, through its failure to implement reasonable data retention procedures, Defendant retained significantly more data than was needed, thereby unnecessarily enlarging the harmful effects of the Data Breach to include victims from as far back as 1954.

151. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class Members, Defendant prevented Plaintiffs and Class Members from taking meaningful, proactive steps to securing their PII and mitigating damages.

152. Plaintiffs and Class Members could have taken actions earlier had they been timely notified of the Data Breach.

153. Plaintiffs and Class Members could have enrolled in credit monitoring, could have instituted credit freezes, and could have changed their passwords, among other things, had they been alerted to the Data Breach more quickly.

154. Plaintiffs and Class Members have suffered harm from the delay in notifying them of the Data Breach.

155. As a direct and proximate cause of Defendant's conduct, including but not limited to its failure to implement and maintain reasonable security practices and procedures, Plaintiffs and Class Members have suffered, and/or will suffer injury and damages, including but not limited to:

a. Actual damages in the forms of identity theft and fraud;

b. The loss of the opportunity to determine for themselves how their PII is used;

c. The publication and/or theft of their PII;

d. Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, including the need for substantial credit monitoring and identity protection services for an extended period of time;

e. Lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft;

f. Costs associated with placing freezes on credit reports and password protections;

g. Anxiety, emotional distress, loss of privacy, and other economic and non-economic losses;

h. The continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of employees in its continued possession; and

i. Future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives. Thus, Plaintiffs and the Class are entitled to damages in an amount to be proven at trial.

156. The damages Plaintiffs and the Class have suffered (as alleged above) and will suffer are the direct and proximate result of Defendant's negligent conduct.

157. Plaintiffs and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

B. COUNT II – NEGLIGENCE PER SE

158. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

159. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems, data security, and data retention policies to properly safeguard the PII of Plaintiffs and the Class.

160. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as CEI, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

161. As a condition of employment, Plaintiffs and the Class Members were obligated to provide Defendant with their PII.

162. Defendant violated the FTCA by failing to use reasonable measures to protect the PII of Plaintiffs and the Class and not complying with applicable industry standards, as described herein.

163. Defendant breached its duties to Plaintiffs and the Class under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

164. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

165. Plaintiffs and the Class are within the class of persons that the FTCA was intended to protect.

166. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against.

167. Defendant breached its duties to Plaintiffs and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and the Class Members' PII.

168. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, damages arising from the Data Breach by, *inter alia*, experiencing actual misuse of their PII in the forms of identity theft and fraud; having to spend time reviewing their accounts and credit reports for unauthorized activity; spending time and incurring costs to place and re-new a "freeze" on their credit; spend time and effort cancelling their accounts; be inconvenienced by the credit freeze, which requires them to spend extra time unfreezing their account with each credit bureau any time they want to make use of their own credit; and becoming a victim of identity theft, which may cause damage to their credit and ability to obtain insurance, medical care, and jobs.

169. The injury and harm that Plaintiffs and Class Members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

C. COUNT III – BREACH OF IMPLIED CONTRACT

170. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

171. Defendant offered employment, compensation, and other elective benefits to Plaintiffs and the Class Members in exchange for their PII and labor.

172. Defendant required Plaintiffs and the Class Members to provide their PII, including names and Social Security numbers, and other personal information. In exchange Defendant promised to keep the PII of Plaintiffs and Class Members safe from unauthorized access and to delete or destroy the PII once the employment relationship ended, or it was no longer necessary to maintain the PII.

173. Plaintiffs and Class Members, had they known that Defendant would not keep their PII secure or that Defendant would continue to possess it for years after their employment ended, would have demanded higher pay or chosen to take other employment and not be employed by Defendant.

174. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiffs and the Class Members in its possession was only used to provide the agreed-upon compensation and other elective employment benefits from Defendant.

175. These exchanges constituted an agreement between the Parties: Plaintiffs and the Class Members would provide their PII for a limited period of time in exchange for employment and benefits provided by Defendant. No reasonable person would have provided their PII to Defendant without a promise to safeguard it and no reasonable person would have provided their PII to Defendant to retain for its own uses for years after the employment ended.

176. These agreements were made with Plaintiffs as an inducement to being employed by Defendant.

177. It is clear from these exchanges that the parties intended to enter into an agreement. Plaintiffs and the Class Members would not have disclosed their PII to Defendant but for Defendant's promise of compensation and other employment benefits and Defendant's promise to safeguard and delete their PII. Defendant presumably would not have taken Plaintiffs' and Class Members' PII if it did not intend to provide Plaintiffs and the Class Members compensation and other employment benefits. Nor could Defendant reasonably infer from the circumstances of the transaction that safeguarding

the PII was not a necessary obligation or that it could maintain the PII for purposes unrelated to employment, i.e., after the relationship ended.

178. Defendant was therefore required to reasonably safeguard and protect the PII of Plaintiffs and the Class Members from unauthorized disclosure and/or use and to delete it following the end of the employment relationship.

179. Plaintiffs and the Class Members accepted Defendant's employment offer and fully performed their obligations under the implied contract with Defendant by providing their PII, directly or indirectly, to Defendant, among other obligations.

180. Plaintiffs and the Class Members would not have provided and entrusted their PII to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their PII for uses other than compensation and other employment benefits from Defendant.

181. Plaintiffs and the Class Members did not provide their PII for non-employment purposes and Defendant had no reason to retain it following the end of the employment term.

182. Defendant breached its implied contracts with the Plaintiffs and the Class Members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' PII.

183. Defendant also breached its implied contracts with Plaintiffs and Class Members by retaining PII following the end of Plaintiffs' and Class Members' employment term, including employees from 1954.

184. Defendant's failure to implement adequate measures to protect the PII of Plaintiffs and Class Members violated the purpose of the agreement between the parties: Plaintiffs' and Class Members' employment in exchange for compensation and benefits.

185. Defendant was on notice that its systems could be vulnerable to unauthorized access yet failed to invest in proper safeguarding of Plaintiffs' and Class Members' PII.

186. Instead of spending adequate financial resources to safeguard Plaintiffs' and Class Members' PII, which Plaintiffs and the Class Members were required to provide to Defendant, Defendant instead used that money for other purposes, thereby breaching its implied contracts it had with Plaintiffs and Class Members.

187. Plaintiffs and the Class Members did all or substantially all the significant things that the contract required them to do.

188. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiffs and Class Members, Plaintiffs and the Class Members suffered injury as described in detail in this complaint and are entitled to damages in an amount to be proven at trial.

189. The losses and damages Plaintiffs and Class Members sustained (as described above) were the direct and proximate result of Defendant's breach of the implied contract with Plaintiffs and Class Members.

D. COUNT IV – UNJUST ENRICHMENT

190. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

191. This count is plead in the alternative to Count III (Breach of Implied Contract).

192. The Plaintiffs and the Class Members conferred a monetary benefit on Defendant by providing their PII which Defendant required as a condition of their employment. The Plaintiffs and Class Members provided their PII and accepted employment on the condition that Defendant safeguard their PII and deleted it once it was no longer required to retain it.

193. The Plaintiffs and Class Members conferred a monetary benefit on Defendant in that Defendant derived revenue from their labor, a precondition of which required Plaintiffs and the Class Members to entrust their PII to Defendant. Without the labor and PII provided by Plaintiffs and Class Members, Defendant could not derive revenue from its regular business activities. A portion of the revenue derived from the labor and PII of the Plaintiffs and Class Members was to be used to provide a reasonable level of data security and practices, and the amount of revenue to be allocated to data security is known to Defendant.

194. Defendant knew that the Plaintiffs and Class Members conferred a benefit on it and Defendant accepted that benefit. Defendant derived revenue from the labor and PII of Plaintiffs and the Class and rather than use a portion of that revenue to protect the PII of Plaintiffs and the Class it instead diverted that money to its own profit.

195. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Member's PII. Instead of providing a reasonable level of security that would have prevented the

hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

196. Under the principles of equity and good conscience, Defendant should not be permitted to retain the profits it wrongfully derived from the Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

197. Defendant failed to secure Plaintiffs' and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided. Defendant has money in its hands that in equity and good conscience, it should not be permitted to retain.

198. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged and that it diverted money intended to protect Plaintiffs and the Class to its own profits.

199. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their PII, they would not have agreed to provide their PII or labor to Defendant.

200. The Plaintiffs and Class Members have no adequate remedy at law.

201. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft and fraud; (b) the loss of the opportunity of how their PII is used; (c) the

compromise, publication, and/or theft of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of the Plaintiffs and Class Members.

202. As a direct and proximate result of Defendant's conduct, the Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

203. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of the Plaintiffs and Class members, proceeds that they unjustly received from them.

E. COUNT V – CALIFORNIA UNFAIR COMPETITION LAW, Cal. Bus. & Prof. Code § 17200, *et seq.*

204. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

205. Defendant violated Cal. Bus. Prof. Code § 17200 et seq. by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200, including but not limited to the following:

a. Defendant engaged in deceptive acts and practices by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard employees' PII from unauthorized disclosure, release, data breach, and theft; representing and advertising that they did and would comply with the requirement of relevant federal and state laws pertaining to the privacy and security of the Plaintiffs' and Class Member's PII; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Plaintiffs' and Class Members' PII.

b. Defendant engaged in unfair acts and practices by establishing the substandard security practices and procedures described herein; by collecting the Plaintiffs' and Class Members' PII as a condition of their employment with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and Class Members' PII in an unsecure electronic environment. These unfair acts and practices were immoral unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and Class Members. Defendant's practice was also contrary to legislatively declared and

public policies that seek to protect consumer data and ensure that entities who collect or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTCA, 15 U.S.C. § 45.

c. Defendant engaged in unfair acts and practices with respect to the collection of the Plaintiffs' and Class Members' PII by failing to disclose the Data Breach in a timely and accurate manner.

206. As a direct and proximate result of Defendant's unfair and unlawful practices and acts, Plaintiffs and the Class were injured and lost money or property, including but not limited to the overpayments Defendant received to take reasonable and adequate security measures (but did not), the loss of their legally protected interest in the confidentiality and privacy of their PII, and additional losses described above.

207. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Class.

208. Plaintiffs seek relief under Cal. Bus. & Prof. Code § 17200, et seq., including restitution to the Class of money or property that the Defendant may have acquired by means of Defendant's deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. Pro. § 1021.5), and injunctive or other equitable relief.

F. COUNT VI – INJUNCTIVE / DECLARATORY RELIEF

209. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

210. As previously alleged and pleaded, Defendant owes duties of care to the Plaintiffs and Class Members that require it to adequately secure their PII.

211. Defendant still possesses the PII of the Plaintiffs and the Class Members even after their employment relationship ended and Defendant was no longer required to maintain it.

212. Defendant has not satisfied its obligations and legal duties to the Plaintiffs and the Class Members.

213. According to the Notice, Defendant is taking some steps to increase its data security, but it is unclear whether those steps are adequate or whether Defendant intends to continue retaining ex-employee PII. Moreover, there is nothing to prevent Defendant from reversing these changes once it has weathered the increased public attention resulting from this Data Breach, and to once again place profits above protection.

214. The Plaintiffs, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) to comply with its obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering Defendant to engage third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering Defendant to significantly increase its spending on cybersecurity, including systems and personnel;

c. Ordering Defendant to engage third-party security auditors and internal personnel to run automated security monitoring;

d. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner any PII not necessary for its provisions of services;

f. Ordering that Defendant conduct regular database scanning and securing checks;

g. Ordering Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

h. Ordering Defendant to implement and enforce adequate retention policies for PII, including destroying PII as soon as it is no longer necessary for it to be retained;

i. Ordering Defendant to meaningfully educate its employees about the threats they face because of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves; and

j. Ordering that Defendant remove former employees' PII from any hard drive or server that has external (Internet) access.

VIII. PRAYER FOR RELIEF

WHEREFORE, the Plaintiffs and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiffs is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual damages, punitive damages, attorney fees, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Plaintiffs and Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of the Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

/////

/////

/////

/////

/////

/////

/////

IX. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all appropriate issues raised in this Complaint.

DATED: February 1, 2024

GREEN & NOBLIN, P.C.
By: *s/ Robert S. Green*

Robert S. Green
Evan E. Sumer
1 Blackfield Drive, No. 360
Tiburon, CA 94920

Telephone: (415) 477-6700
Facsimile: (415) 477-6710
Email: gnecf@classcounsel.com

William B. Federman
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
-and-
212 W. Spring Valley Rd.
Richardson, TX 75081
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
Email: wbf@federmanlaw.com

Daniel Srourian, Esq.
SROURIAN LAW FIRM, P.C.
3435 Wilshire Blvd., Suite 1710
Los Angeles, California 90010
Telephone: (213) 474-3800
Facsimile: (213) 471-4160
Email: daniel@slfla.com

Attorneys for Plaintiffs and the Proposed Class